Investigación

Algoritmo esteganográfico de clave privada

Steganographic algorithm of private key

Anier Soria Lorente, Rayner Manuel Sánchez Reyes
y Andys Marcos Ramírez Aberasturis

Revista de Investigación

G.I.E Pensamient Matemàtic

Volumen III, Número 2, pp. 059–072, ISSN 2174-0410
Recepción: 24 Feb'13; Aceptación: 31 Jun'13

1 de octubre de 2013

Resumen

La esteganografía con clave privada, es un sistema similar a sistemas criptográficos de cifras simétricas. En este artículo se presenta un nuevo algoritmo esteganográfico, el cual utiliza una clave privada, que permite generar una secuencia binaria pseudoaleatoria, indicando así los píxeles de la imagen donde serán insertados los elementos de la secuencia binaria del mensaje secreto. El algoritmo propuesto, mejora en cuanto al nivel de imperceptibilidad respecto al método de los bits menos significativos[1].

Palabras Clave: Esteganografía, Criptografía, Esteganograma, Clave privada.

Abstract

The steganography with private key, is a similar system to cryptographic systems of symmetric ciphers. In this paper a new steganographic algorithm is presented, which uses a private key, that it permits generating a binary pseudo-random sequence, indicating thus the pixels of the image where the elements of the binary sequence of the secret message will be inserted. The proposed algorithm, improves as to the level of imperceptibility in relation to the method of least significant bits[2].

Keywords: Steganography, Cryptography, Steganogram, Private key.

1. Introducción

Hoy en día la comunicación está estrechamente vinculada a internet y sin duda alguna se ha convertido en parte de la infraestructura del mundo moderno. Este hecho, ha posibilitado

[1] El método de los bits menos significativos, indica el procedimiento esteganográfico que a través de una operación lineal, se encarga de ocultar información en el bit menos significativo de cada byte de algún medio digital.

[2] The method of least significant bits, indicate the steganographic procedure than through a linear operation, it's entrusted of hiding information in the least significant bit of each byte of some digital medium.

que la información transite mediante disímiles medios de comunicación, siendo utilizada en considerables aplicaciones en la ciencia, en la ingeniería, en la industria etc… En general, se inquiere que la comunicación se realice de manera privada y segura, lo cual ha llevado consigo que los mecanismos de seguridad de la información cobren cada vez mayor importancia y sean desarrollados con gran prontitud. Con el transcurso del tiempo la seguridad en los ordenadores ha jugado un rol fundamental en nuestra sociedad, la cual se rige por la comunicación y el intercambio de información mediante Internet, siendo la comunicación e información partes fundamentales para su desarrollo.

El masivo almacenamiento de información en forma digital mediante soporte electrónico, unido al enorme desarrollo de las comunicaciones, ha propiciado un modo de trabajo y de vida del que difícilmente podríamos ya sustraernos. Los medios para el almacenamiento y la transmisión de información están disponibles a muchos y a un bajo coste. Podemos acceder de modo masivo e inmediato a diferentes bases de datos ubicadas en diferentes puntos del mundo. La sociedad demanda nuevos servicios de comunicación: banco por la red, comercio, firma digital con valor mercantil, etc.; se exige confidencialidad, integridad y accesibilidad a la información.

Existen, sin embargo, muchos problemas todavía no del todo resueltos en este universo de las comunicaciones. Existe el peligro de que nuestra información, muchas veces confidencial, pueda ser accedida por personas no deseadas: consultada, modificada, destruida; también podemos ser perjudicados de forma que se desbarate, por un agente externo, los protocolos de autorizaciones, siendo impedidos a acceder a nuestra propia información. La información en tránsito es fácilmente interceptada. Frente al deseo de confidencialidad podemos sufrir un ataque de interceptación; frente al deseo de autenticación podemos ser suplantados; frente al deseo de integridad de nuestra información podemos sufrir modificaciones e incluso destrucción de nuestra información; frente al deseo de autenticidad podemos sufrir ataques de falsificación. Es por ello que se han adoptado diferentes formas para la protección de la información, ya que los riesgos de ser interceptada son muy altos, pudiendo así ser plagiada o modificada. Por tal motivo el uso de la Criptografía y la Esteganografía [1, 2, 3, 7, 10, 17] ha jugado un papel significativo para la seguridad de la información.

La esteganografía consiste en ocultar en el interior de una información, aparentemente inocua, otro tipo de información (cifrada o no), de manera tal, que se puede definir la esteganografía como el conjunto de técnicas que permiten ocultar cualquier tipo de información de tal forma que la presencia de un mensaje no pueda ser detectada [11]. De modo que la esteganografía constituye un conjunto de técnicas las cuales permiten ocultar o camuflar cualquier tipo de datos dentro de información considerada como válida, en cuanto a este artículo imágenes digitales. La esteganografía permite burlar la vigilancia electrónica en Internet, o simplemente que terceras personas no tengan acceso a dicha información. Con el avance de la informática y de Internet se ha propiciado un marco ideal para que los métodos esteganográficos alcancen un elevado auge. La esteganografía actual, se basa en ocultar información binaria en los bits que juegan un papel redundante en un archivo. Los bits que forman el mensaje a ocultar se insertan en el archivo ya existente, procurando que el resultante después de la inserción sea similar al original.

La esteganografía utiliza medios digitales, tales como archivos de texto, audio, imagen y video [5, 6, 7, 8, 14], que son utilizados como el archivo de transporte para ocultar la información, a este medio se le conoce como contenedor, cubierta o estego-medio. Cuando el mensaje secreto es ocultado en el estego-medio mediante una técnica esteganográfica se obtiene un esteganograma que contendrá el mensaje oculto en el estego-medio. Luego una vez que los datos han sido ocultados, la información puede ser transferida a través de los medios de comunicación inseguros.

Entre las técnicas más usadas en la esteganografía se encuentra las correspondientes al dominio espacial [4]. El sistema matricial de coordenadas de una imagen es lo que se denomina

dominio espacial, de manera que el término dominio espacial se refiere al conjunto de píxeles que componen a una imagen. La aplicación de la esteganografía en el dominio espacial, radica en que los algoritmos son utilizados en la manipulación de los píxeles y en la inserción de la información secreta en los bits menos significativos o bien de mayor redundancia. Los métodos del dominio espacial implican la generación de una nueva imagen modificando el valor del píxel en una simple localización, basándose en una regla global aplicada a cada localización de la imagen original. El proceso consiste en obtener el valor del píxel de una localización dada en la imagen, modificándolo por una operación lineal o no y colocando el valor del nuevo píxel en la correspondiente localización de la nueva imagen. El proceso se repite para todas y cada una de las localizaciones de los píxeles en la imagen.

Otra de las técnicas dentro de la esteganografía tiene que ver con el dominio de la frecuencia, la cual está vinculada a los cambios de las altas y bajas frecuencias de la imagen, de forma tal, que las altas frecuencias como los bordes, las líneas y ciertos tipos de ruidos son utilizados para ocultar información. Dentro de esta técnica se utilizan transformadas tales como la de Fourier [13], la transformada discreta de los cosenos [6, 14, 19, 20] y la de wavelets [5, 6, 15, 18]. Existen otros trabajos de gran relevancia dentro de la esteganografía, los cuales se pueden encontrar en [9, 12, 16, 19, 21].

En este artículo se presenta un nuevo algoritmo correspondiente al dominio espacial, el cual se expondrá en la próxima sección. Además, el mismo hace uso de una clave privada que propiciará el mensaje secreto sólo a aquel receptor que porte de la misma; dicha clave genera una secuencia binaria pseudoaleatoria, que indica aquellos píxeles de la imagen, donde serán insertados los elementos de la secuencia binaria del mensaje secreto. Para finalizar, en la última sección, se expondrán los resultados conseguidos a partir de dicho algoritmo y luego se darán las conclusiones a las que fueron arribadas.

2. Desarrollo del algoritmo esteganográfico

Una clave privada en un sistema esteganográfico es similar al cifrado simétrico, donde el remitente escoge un estego-medio y oculta el mensaje mediante una clave privada. De forma tal, que si la clave privada utilizada para ocultar la información secreta es conocida por el receptor, el mismo puede extraer la información secreta mediante el proceso de extracción. Evidentemente, la esteganografía de clave privada requiere del intercambio de dicha clave, aquí es precisamente, donde entra a jugar un papel fundamental, la criptografía asimétrica o de clave pública [10][3]. A continuación se describen los pasos necesarios para implementar el algoritmo propuesto en este artículo, véase la figura 1. Nótese que en el algoritmo que sigue a continuación, se omite el paso de transformar el mensaje secreto en una secuencia binaria, así como la entrada de la imagen original o estego-imagen por parte del usuario, pues claramente estos pasos se encuentran de forma implícita.

2.1. Proceso de inserción

1.- Procesar la clave.

1.1.- Solicitar una clave de 64 bits al usuario. La clave se puede introducir directamente o puede ser el resultado de alguna operación anterior.

1.2.- Calcular 15 subclaves.

[3] La criptografía asimétrica o de clave pública es el método criptográfico, que utiliza un par de claves para el intercambio de información. Ambas claves pertenecen al emisor; una de ellas es pública y la otra es totalmente privada. Además, los métodos criptográficos garantizan que este dúo de claves sólo se pueda generar una vez, de modo que se puede asumir que no es posible que dos personas o entidades hayan obtenido casualmente la misma pareja de claves.

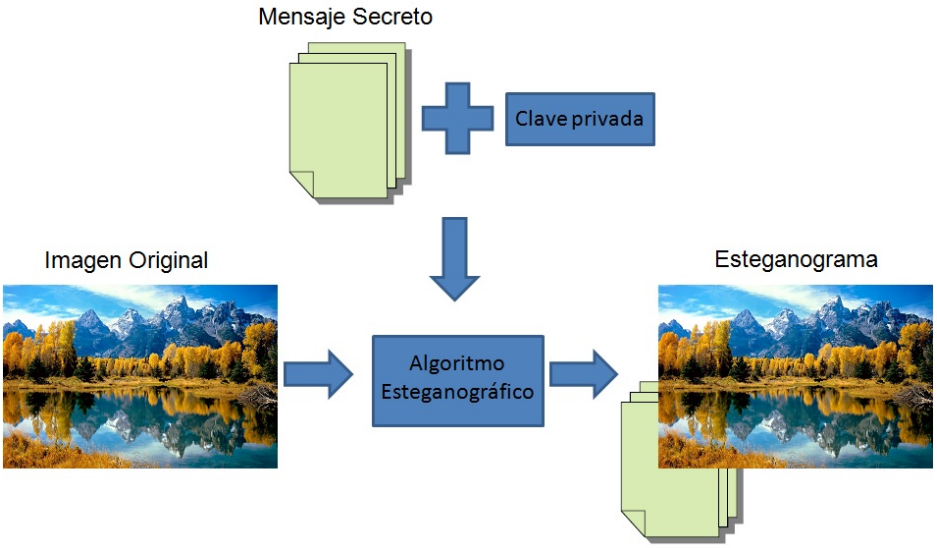

Figura 1. Proceso de inserción.

1.2.1.- De cada uno de los ocho bytes de la clave entrada por el usuario se elimina el octavo bit, el menos significativo. Para ello hay que realizar la siguiente permutación en la clave de 64 bits

45	21	60	12	23	49	33	5
62	57	3	38	1	19	54	9
15	20	7	50	43	4	46	31
58	36	53	22	41	35	29	55
27	14	44	63	6	51	34	11
42	28	61	17	13	37	52	30
10	39	25	2	59	18	26	47

reduciéndose la misma a 56 bits. El bit 1, el más significativo de la clave transformada, es el bit 45 de la clave original, el bit 2 pasa a ser el bit 21, etc...

1.2.2.- Dividir la clave permutada en dos mitades de 28 bits cada una, $c_1^{(1)}$ el bloque que contiene los 28 bits de mayor peso y $c_1^{(2)}$ los 28 bits restantes.

1.2.3.- Calcular las 15 subclaves, comenzando a partir de $i = 1$.

1.2.3.1.- Rotar 1 o 2 bits a la izquierda de $c_i^{(1)}$ y $c_i^{(2)}$ para conseguir $\tilde{c}_i^{(1)}$ y $\tilde{c}_i^{(2)}$ respectivamente. El número de bits de desplazamiento está dado mediante $1+\mathrm{mod}(i-1,2)$, $i = 1,\ldots,15$.

1.2.3.2.- Concatenar $\tilde{c}_i^{(1)}$ y $\tilde{c}_i^{(2)}$ y permutar el resultado mediante la correspondiente compresión $\mathrm{mod}(i,2)$

30	52	7	19	39	55	28	13
4	18	53	29	47	9	32	6
43	24	40	17	50	2	15	1
5	27	54	14	49	37	38	22
31	12	48	23	33	10	26	25
42	3	41	34	8	35	51	11

37	34	15	23	48	22	42	47
49	54	43	24	55	3	35	40
19	11	14	44	10	29	45	52
21	25	31	9	41	28	33	1
13	32	4	51	17	8	39	30
27	38	20	12	5	53	50	7

De esta manera se obtiene la subclave C_i, que tiene una longitud de 48 bits.

1.2.3.3.- Regresar a 1.2.3.1, hasta que se haya calculado la última subclave C_{15}.

2.- Conseguir una secuencia binaria cuya cantidad de bits iguales a 1 coincida con la longitud de la secuencia binaria del mensaje secreto. Para ello se deben seguir los siguientes pasos:

2.1.- Hacer $k = 1$. Denotar el número de bits de la secuencia binaria de la clave introducida por el usuario mediante NumBits1.

2.1.1.- Aplicar la correspondiente expansión $\mathrm{mod}(\mathrm{NumBits1}, 8)$

37	17	9	10	40	23	14	18
3	42	39	35	15	32	24	28
12	22	48	47	19	7	44	16
30	27	20	42	25	33	2	31
4	23	12	5	26	21	38	43
41	34	3	7	1	11	31	37
6	36	29	45	46	13	28	17
27	19	11	8	3	29	1	47

(1)

47	1	39	2	48	40	31	11
9	18	3	23	21	8	35	25
31	14	20	12	38	37	16	27
36	46	7	17	32	48	10	33
34	15	28	22	24	2	42	5
23	29	43	13	41	26	12	39
45	27	29	11	44	30	17	4
18	37	1	19	7	9	6	47

(2)

13	48	15	29	37	10	24	5
11	7	47	21	12	27	3	35
21	41	31	44	30	19	39	23
2	34	17	25	22	46	36	31
33	43	9	4	14	28	17	4
7	11	3	8	32	19	47	26
40	23	45	38	6	12	42	8
18	42	37	12	4	16	20	2

(3)

17	8	18	38	11	42	21	1
29	46	23	47	31	39	43	35
23	28	17	37	22	45	7	20
13	33	15	32	6	44	29	12
37	16	27	26	21	5	34	36
9	3	11	10	2	27	40	31
30	15	19	48	8	3	12	4
37	47	1	24	7	25	14	41

(4)

7	22	38	18	33	26	48	39
8	45	28	42	35	24	32	12
27	47	21	13	2	9	23	42
46	3	41	10	14	41	37	11
11	34	7	31	1	27	17	3
30	31	36	17	21	12	19	44
47	29	40	38	23	29	16	4
5	20	6	15	43	37	1	25

(5)

29	35	12	11	9	41	24	14
29	15	1	19	32	22	18	27
33	25	43	1	2	23	45	31
5	40	47	17	38	39	17	37
36	21	13	7	3	16	28	48
21	6	31	44	30	38	10	12
34	7	8	4	27	42	46	26
42	20	23	41	11	3	47	37

(6)

23	36	16	44	39	12	19	2
35	46	33	20	3	7	29	8
13	18	5	14	17	22	31	47
34	40	27	4	48	41	37	12
27	31	6	30	28	43	47	42
21	41	23	3	17	38	1	7
26	24	21	42	9	10	15	45
32	11	1	37	38	11	25	29

(7)

20	1	10	47	7	29	4	16
37	19	35	9	37	41	44	26
30	23	25	15	24	2	12	11
14	38	22	8	38	42	48	7
47	46	5	17	31	39	23	27
3	33	6	28	18	21	1	17
42	34	43	41	13	11	45	29
36	3	32	27	21	40	12	31

(8)

a la secuencia binaria $C_k \oplus C_{k+1}$ extendiendo la misma a una secuencia binaria de 64 bits, donde $\oplus$ es la siguiente operación binaria ($0 \oplus 0 = 1 \oplus 1 = 0$ y $0 \oplus 1 = 1 \oplus 0 = 1$).

2.1.2.- Denotar por seq1 al resultado conseguido en 2.1.1.

2.2.- Mientras que la cantidad de bits iguales a 1 en la secuencia binaria seq1 sea menor a la longitud de la secuencia binaria del mensaje, proseguir.

2.2.1.- Si $k < 14$ entonces:

2.2.1.1- Hacer $k = k + 1$.

2.2.1.2- Concatenar seq1 con la secuencia binaria resultante de aplicar la correspondiente expansión $\mathrm{mod}(\mathrm{NumBits1}, 8)$ de (1)-(8) a $C_k \oplus C_{k+1}$.

2.2.1.3.- Tomar seq1 como el resultado conseguido en 2.2.1.2.

2.2.2.- Si no se cumple la condición 2.2.1, entonces concatenar la subclave C_{15} con los dos bytes intermedios de la subclave C_{14} formando así una nueva clave de 64 bits y luego a partir de la misma generar 15 subclaves usando los pasos de 1.2 hasta 1.2.3.3.

2.2.2.1.- Luego, hacer $k = 1$.

2.2.2.2.- Aplicar el paso 2.2.1.2.

2.2.2.3.- Tomar seq1 como el resultado conseguido en 2.2.2.2. Proseguir de esta manera hasta que se cumpla la condición 2.2.

2.3.- Extraer la sub-secuencia binaria de seq1 partiendo de su primer bit, cuya cantidad de bits iguales a 1 sea exactamente la longitud de la secuencia binaria del mensaje secreto.

3.- Hacer seq2 igual a la secuencia binaria resultante del paso 2.3. Si la longitud de la secuencia seq2 es menor ó igual que $3mn$ (siendo m y n las dimensiones de la imagen original), entonces proseguir de la siguiente manera.

3.1.- Recorrer cada uno de los bytes de cada píxel de la imagen original e insertar en los correspondientes bits menos significativos, los bit de la secuencia binaria del mensaje secreto, siempre y cuando, el correspondiente bit de la secuencia seq2 sea igual a 1, este proceso se extiende hasta el último bit de la secuencia seq2. Es decir, la secuencia seq2 controla e indica la localización del bit menos significativo de cada byte de la imagen original, donde se insertará el bit de la secuencia binaria del mensaje secreto.

2.2. Proceso de extracción

El proceso de extracción se realiza del siguiente modo: el receptor debe conocer la clave compuesta por aquella mediante la cual se ocultó el mensaje secreto en la imagen original y la longitud de la secuencia binaria de dicho mensaje. Luego, se debe realizar el mismo proceso dado por los pasos del 1 hasta el 2.3, para así conseguir la secuencia binaria seq2 e inmediatamente, a partir de la misma, extraer el mensaje secreto oculto dentro del esteganograma. Para ello, se debe recorrer cada uno de los bytes de cada píxel del esteganograma hasta terminada la longitud de la secuencia binaria seq2 y en cada paso donde el bit de seq2 sea igual a 1, extraer el bit menos significativo del correspondiente byte, véase la figura 2.

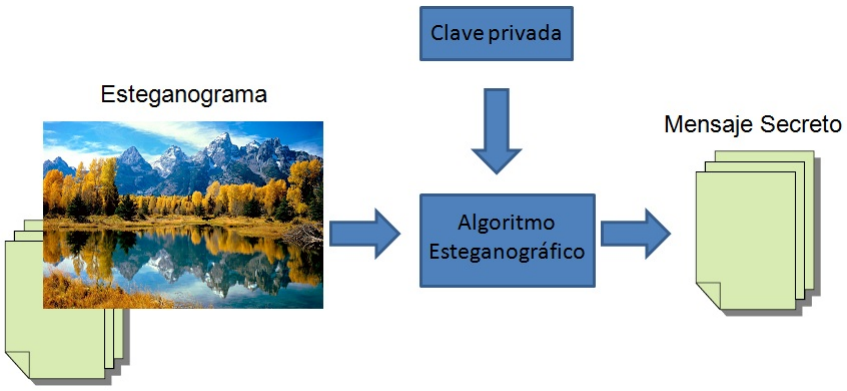

Figura 2. Proceso de extracción.

3. Evaluación y Resultados

En esta sección se presentan las evaluaciones y resultados del algoritmo esteganográfico propuesto.

La eficiencia en la protección de la información mediante la esteganografía, radica precisamente en el uso de un algoritmo adecuado que posibilite de forma correcta la inserción de

datos, donde uno de los principales factores a tener en cuenta es el nivel de imperceptibilidad, debido a que un sistema esteganográfico tiene que generar un esteganograma suficientemente inocente, ya que no debe de levantarse ninguna sospecha. Por tanto, el grado de distorsión o imperceptibilidad de un esteganograma respecto a la imagen original juega un papel fundamental.

Una medida de distorsión es la conocida PSNR (Relación Señal a Ruido Pico) en el esteganograma con respecto a la imagen original. El PSNR es muy común en el proceso de una imagen, su utilidad reside en dar una relación del grado de supresión de ruido entre la imagen original y el esteganograma, proveyendo de esta manera una medida de calidad. El PSNR está dado en unidades llamadas decibelios (dB) y se escribe de la siguiente forma

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{256^2}{\mathrm{MSE}}\right),$$

donde MSE está dado por el error cuadrático medio

$$\mathrm{MSE} = \frac{1}{3mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{3}\|I(i,j,k) - E(i,j,k)\|^2,$$

siendo I la imagen original y E el esteganograma.

A continuación, se mostrarán algunos de los experimentos realizados a imágenes RGB de 24 bits, donde se puede observar a simple vista, que la imagen original y el esteganograma no muestran diferencias significativas. Además, como se podrá notar, el nivel de imperceptibilidad de los esteganogramas generados a partir del algoritmo propuesto, mejora cuantitativamente respecto al conseguido a partir del método de los bits menos significativos; y esto es comprobable, a través de los correspondientes PSNR en cada uno de los experimentos, véase las figuras (3, 4, 5, 6, 7, 8).

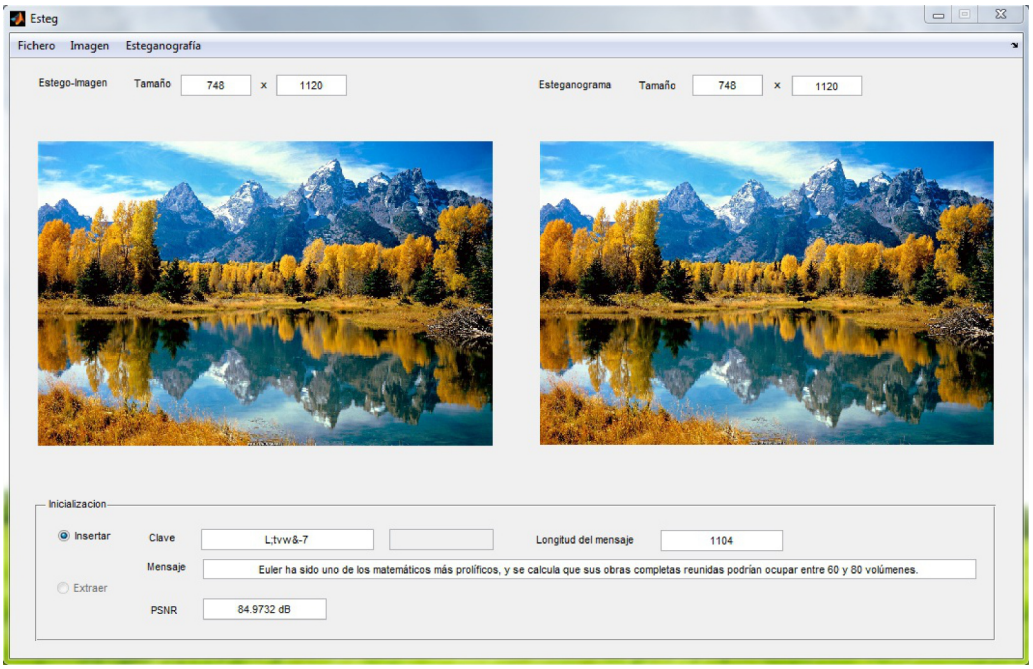

Figura 3. A la izquierda se muestra la imagen original mientras que a la derecha se muestra el esteganograma para la clave privada `L;tvw&-7`.

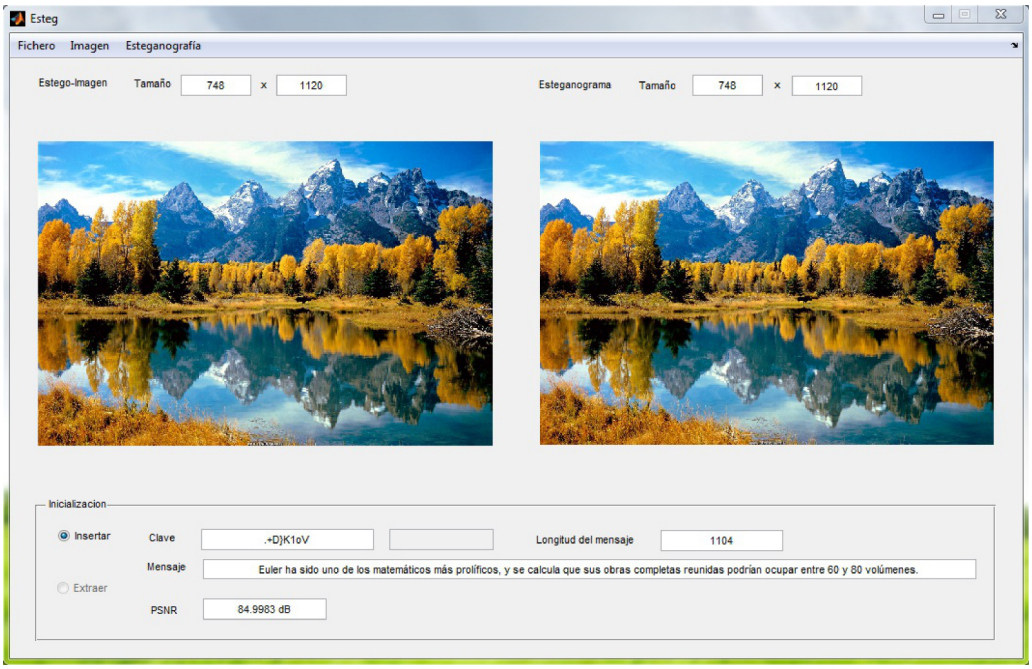

Figura 4. A la izquierda se muestra la imagen original mientras que a la derecha se muestra el esteganograma para la clave privada `.+D}K1oV`.

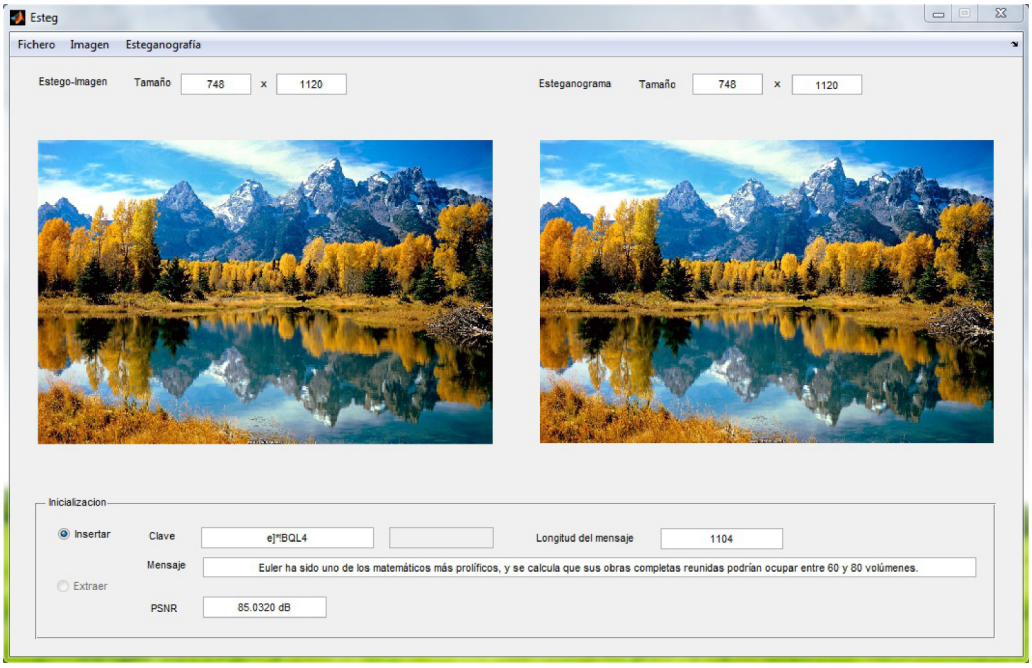

Figura 5. A la izquierda se muestra la imagen original mientras que a la derecha se muestra el esteganograma para la clave privada `e]*!BQL4`.

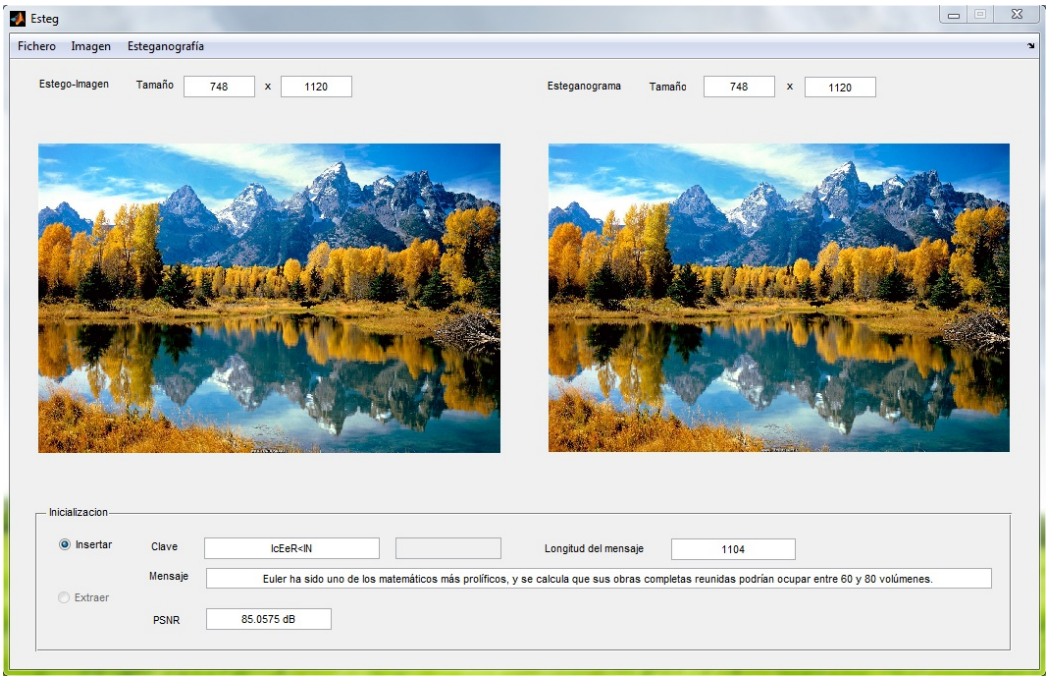

Figura 6. A la izquierda se muestra la imagen original mientras que a la derecha se muestra el esteganograma para la clave privada `IcEeR<IN`.

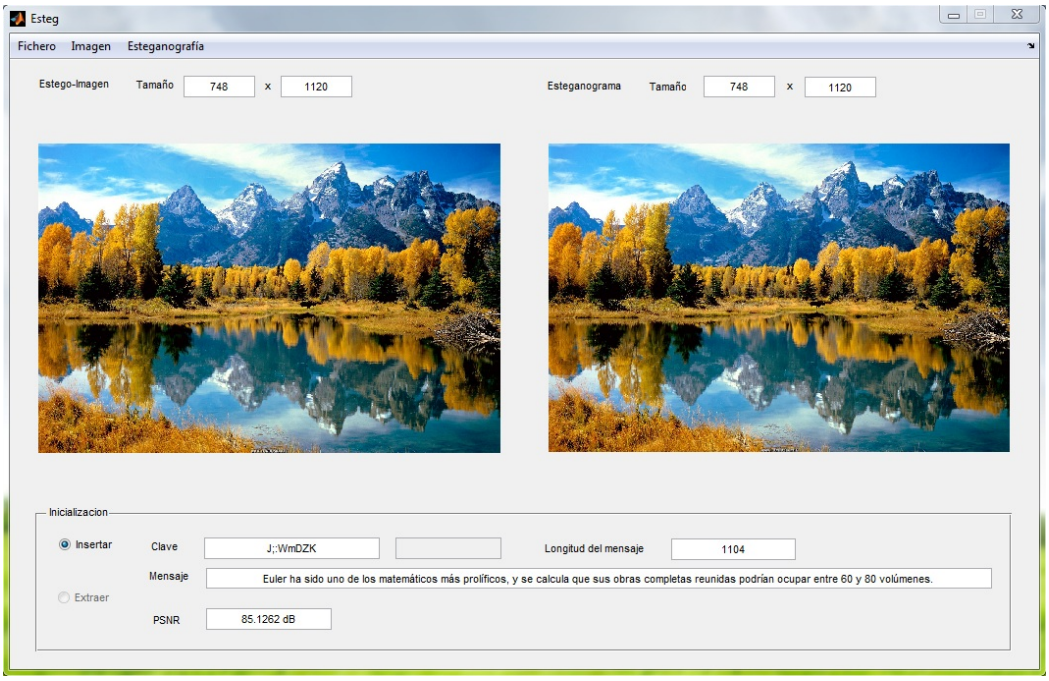

Figura 7. A la izquierda se muestra la imagen original mientras que a la derecha se muestra el esteganograma para la clave privada `J;:WmDZK`.

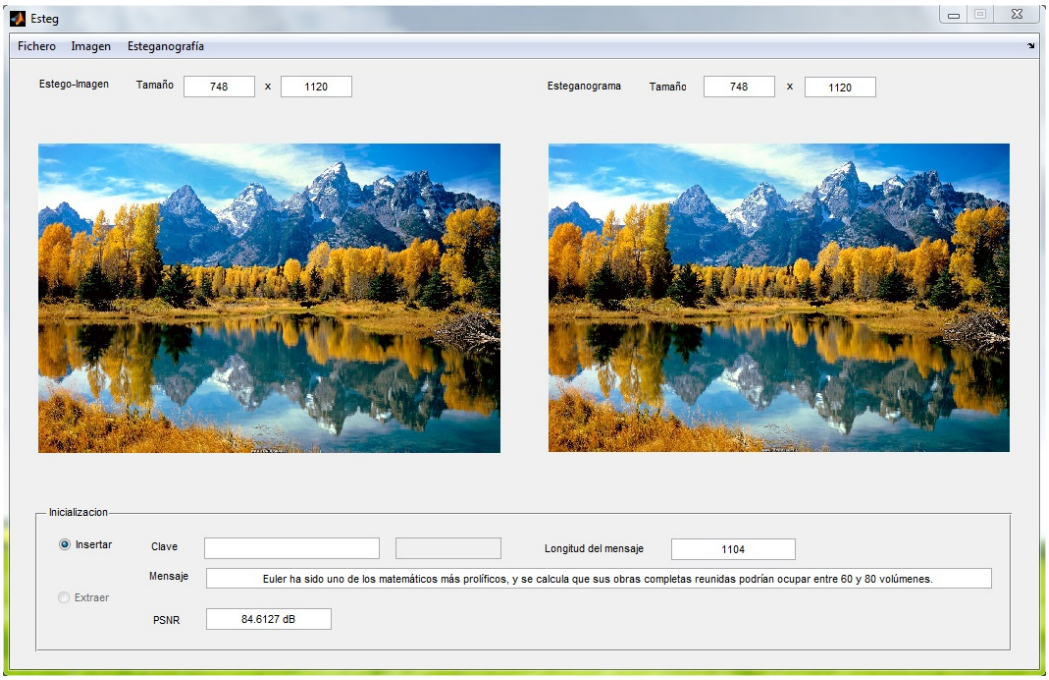

Figura 8. A la izquierda se muestra la imagen original mientras que a la derecha se muestra el esteganograma conseguido a partir del método de los bits menos significativos.

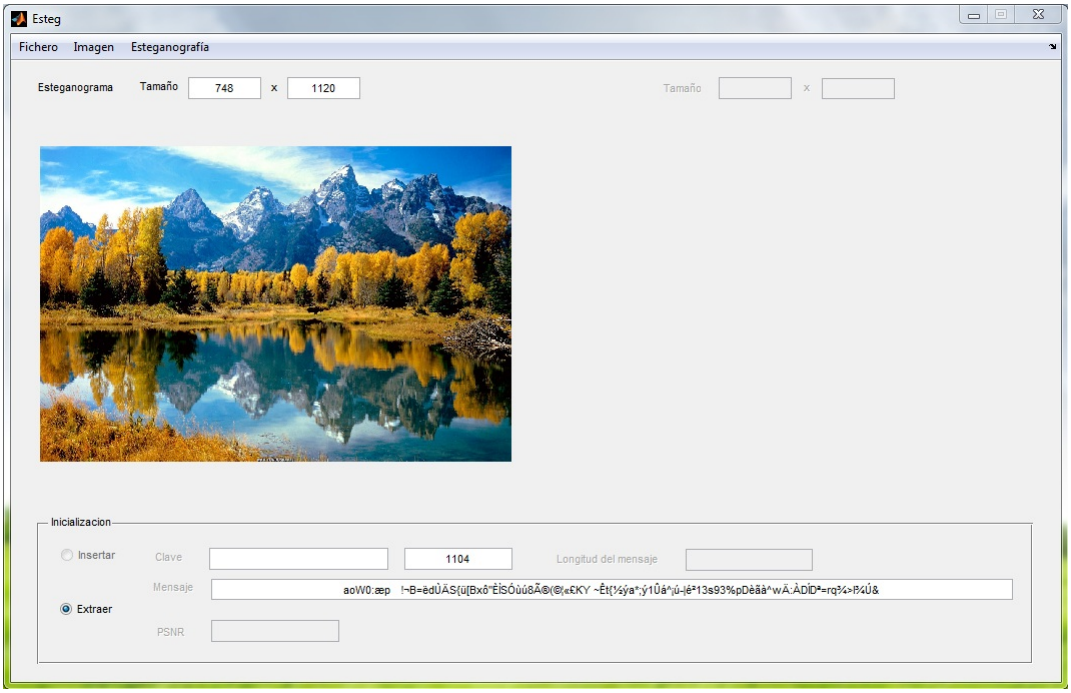

Figura 9. Resultado tras aplicarle a un esteganograma de clave privada el método de los bits menos significativos.

4. Conclusiones

El algoritmo propuesto, permite a través de la clave privada, generar una secuencia binaria pseudoaleatoria, indicando de este modo las posiciones de los píxeles de la imagen, donde

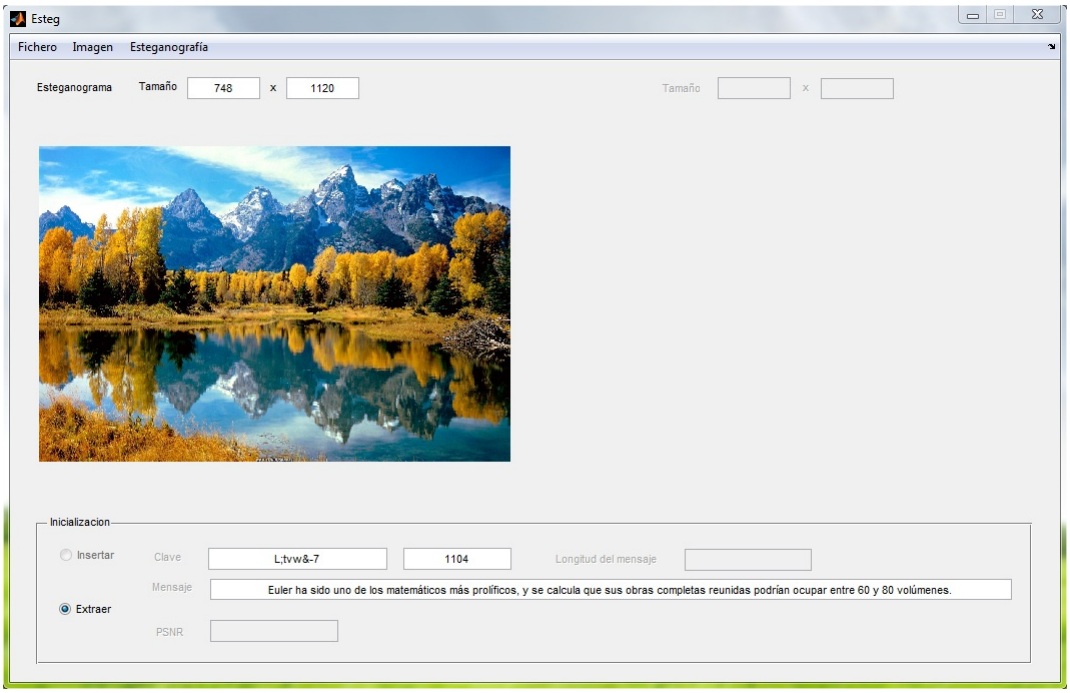

Figura 10. Resultado tras aplicarle al esteganograma de clave privada `L;tvw&-7`*, el algoritmo propuesto para dicha clave.*

serán insertados los elementos de la secuencia binaria del mensaje secreto, posibilitando de esta manera, que no se aglomeren los cambios realizados en la imagen y por consiguiente, dando lugar a que la imagen original y el esteganograma no muestren diferencias notorias.

Nótese que, cada clave privada distribuye de manera distinta los bits de la secuencia binaria del mensaje secreto dentro de la imagen original, obteniéndose así diferentes esteganogramas, lo que constituye una ventaja clara respecto al método de los bits menos significativos, pues si se intentara extraer la información oculta a través de dicho método, el resultado sería un total fracaso, véase la figura 9, sólo se alcanzaría el resultado adecuado, si el receptor porta de la clave privada para poder extraer la información oculta, véase la figura 10. Por lo tanto, el algoritmo esteganográfico aquí propuesto es válido para imágenes RGB de 24 bits.

Referencias

[1] ANDERSON, R. J. and PETITCOLAS, A. P., *On the limits of steganography*, IEEE Journal on Selected Areas in Communications, Vol. 16, Nº 4, pp. 474–481, May 1998.

[2] PETITCOLAS, A. P., ANDERSON, R. J. and KUHN, M., *Information-Hiding:A Survey*, Proc. of the IEEE, Vol. 87, Nº 7, pp. 1019–1022, July 1999.

[3] ARTZ, D., *Digital Steganography: hiding data within data*, IEEE Internet Computing, Vol. 5, Nº 3, pp. 75–80, 2001.

[4] CHANDRAMOULI, R. and MEMON, N., *Analysis of LSB based image steganography techniques*, Proceedings of the International Conference on Image Processing, pp. 1019–1022, 2001.

[5] CARVAJAL-GAMEZ, B. E., FUNES, G. and LOPEZ-BONILLA, J. L., *Esteganografía para Imágenes RGB: Factor de Escalamiento*, Journal of Vectorial Relativity, Vol. 4, Nº 3, pp. 66–77, 2009.

[6] CARVAJAL-GAMEZ, B. E. and LOPEZ-BONILLA, J. L., *Técnica Esteganográfica para ocultar un video dentro de otro utilizando la Transformada Wavelet Discreta*, Journal of Vectorial Relativity, Vol. 4, Nº 2, pp. 54–61, 2009.

[7] CHEDDAD, A., CONDELL, J., CURRAN, K. and MC KEVITT, P., *Digital Image Steganography: Survey and Analyses of Current Methods*, Signal Processing, Vol. 90, Nº 3, pp. 727–752, 2010.

[8] FIORI, D., PONTIN, R. and GOULARTE, R., *Esteganografia em Vídeos: Um Estudo sobre o Estado da Arte*, Instituto de Ciencias Matemáticas e de Computaçao, ISSN: 0103-2569, Nº 292, 2007.

[9] GABRIEL, A. and VALDES, J., *Esteganografía en Dispositivos Móviles*, III Congreso Colombiano de Computación, Medellín, pp. 23–25, 2008.

[10] GONZALEZ, S. and MARTINEZ, C., *Las matemáticas de la seguridad*, ARBOR Ciencia, Pensamiento y Cultura, CLXXXIII 725, ISSN: 0210-1963, pp. 419–425, 2007.

[11] JOHNSON, F. and JAJODIA, S., *Exploring steganography: Seeing the unseen*, IEEE Computer Mag., pp. 26–34, Frebruary 1998.

[12] JOACHIM, J. and BAUML, R., *A Communication Approach to Image Steganography*, Proceedings of SPIE, Vol. 4675, January 2002.

[13] MCKEON, R., *Steganography using the Fourier Transform and Zero-Padding Aliasing Properties*, Member, IEEE, May 2006.

[14] NEELAMANI, R., QUIROZ, R., FAN, Z., DASH, S. and BARANIUK, G., *JPEG Compression history estimation for color images*, IEEE Transactions on Image Processing, Vol. 15, Nº 6, pp. 1365–1378, 2006.

[15] OREA-FLORES, I., ACEVEDO, M. and PLOPEZ-BONILLA, J. L., *Wavelet and Discrete Transform for Inserting Information into BMP Images*, Anziam Journal, Vol. 48, Nº 1, pp. 23–35, 2006.

[16] RADHAKRISNAN, R., KHARRAZI, M. and MEMON, N., *Data Masking: A New Approach for Steganography?*, Journal of VLSI Signal Processing, Vol. 41, pp. 293–303, DOI: 10.1007/s11265-005-4153-1, 2005.

[17] SKORIC, B., *Steganography from weak cryptography*, arXiv:0804.0659v1 [cs.CR] 4, April 2008.

[18] TORRES, S., NAKANO, M. and PEREZ, H., *An image steganography systems based on BPCS and IWT*, Wseas Trans. on Communications, Vol. 5, Nº 6, pp. 814–820, 2006.

[19] TAKAYUKI, I., KAZUMI, Y., HIDEKI, N. and MICHIHARU, N., *Performance improvement of JPEG2000 steganography using QIM*, Journal of Communication and Computer, Vol. 6, Nº 1, pp. 1548–7709, 2009.

[20] VELASCO, C., LOPEZ, J. and NAKANO, M., *Esteganografía en una imagen digital en el dominio DCT*, Científica, Vol. 11, Nº 4, pp. 169–176, 2007.

[21] WESTFELD, A., *A steganographic algorithm*, in Proceedings of the 4th International Workshop on Information Hiding (IH '01), Vol. 2137 of Lecture Notes in Computer Science, pp. 289–302, April 2001.

Sobre los autores:

Nombre: Anier Soria Lorente
Correo electrónico: asorial@udg.co.cu
Institución: Universidad de Granma, Cuba.

Nombre: Rayner Manuel Sánchez Reyes
Correo electrónico: rsanchez@udg.co.cu
Institución: Universidad de Granma, Cuba.

Nombre: Andys Marcos Ramírez Aberasturis
Correo electrónico: andysramirezaberasturis@yahoo.es
Institución: Universidad Carlos III de Madrid, España.